2
Ring Theory

A ring is an algebraic structure on a single underlying set with two binary operations. We will focus on the commutative case where number theory and algebraic geometry provide the keys examples.

2.0 Commutative Rings

2.0.2 Definition. A ***commutative ring*** R is a nonempty set with two binary operations, addition and multiplication, such that
- under addition R is an abelian group;
- multiplication is associative and has an identity denote 1;
- multiplication is distributive: $a(b+c) = ab + ac$ for all $a, b, c \in R$;
- multiplication is commutative: $ab = ba$ for all $a, b \in R$.

Contrary to some conventions, our rings will always have a multiplicative identity 1. Bjorn Poonen (2016) makes a compelling argument for this choice.

2.0.3 Example. Sets of numbers including $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all commutative rings under the usual addition and multiplication. ◇

2.0.4 Example. For any positive integer m, the finite set or quotient $\mathbb{Z}/\langle m \rangle$ is a commutative ring where addition and multiplication are inherited from $\mathbb{Z}$. ◇

2.0.5 Example. Suppose that R is a ring with $1 = 0$. For all $a \in R$, it follows that $a = 1a = 0a = 0$, so R consists of a single element. This is called the ***zero ring***. ◇

2.0.6 Example. Let R be a ring and let X be a nonempty set. The set of maps from X to R equipped with the pointwise addition and multiplication is itself a ring. For all functions $f, g : X \to R$, we have $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. The constant function $x \mapsto 1_R$ is the multiplicative identity. ◇

Many "ring-like" structures without a multiplicative identity do occur, especially in analysis. Focusing on functions with compact support or using convolution as the product are natural examples.

2.0.7 Example. Polynomials in the indeterminate x with coefficients in a ring R also form a ring $R[x]$; addition is defined by

$$\begin{aligned}&(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) + (b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0)\\ &= (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0)\,,\end{aligned}$$

and multiplication is defined by

$$\begin{aligned}&(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0)(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0)\\ &= (a_n b_m)x^{n+m} + (a_n b_{m-1} + a_{n-1}b_m)x^{n+m-1} + \cdots + a_0 b_0 .\end{aligned}$$

In the product, the coefficient of the monomial x^k is the element $\sum_{i=0}^{k} a_{k-i}b_i \in R$. ◇

2.0.8 Example. Formal power series in x with coefficients in a ring R also form a ring $R[[x]]$; addition and multiplication are defined by

$$\left(\sum_{j=0}^{\infty} a_j x^j\right) + \left(\sum_{j=0}^{\infty} b_j x^j\right) = \sum_{j=0}^{\infty}(a_j + b_j)x^j , \quad \text{and} \quad \left(\sum_{j=0}^{\infty} a_j x^j\right)\left(\sum_{j=0}^{\infty} b_j x^j\right) = \sum_{j=0}^{\infty}\left(\sum_{k=0}^{j} a_k b_{n-k}\right)x^j .$$ ◇

2.0.9 Proposition. *Let R be a commutative ring.*

(i) *For all $a \in R$, we have $0a = 0$.*
(ii) *Given the additive inverse $-a$ of $a \in R$, we have $(-1)(-a) = a$.*
(iii) *Given $n \in \mathbb{N}$ such that $n1 = 0$ in R, we have $na = 0$ for all $a \in R$.*
(iv) *For all $a, b \in R$, we have $(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$.*

For any two integer n and k, the ***binomial coefficient*** $\binom{n}{k}$ is defined to be the number of subsets of the set $[n] := \{1, 2, \dots, n\}$ having cardinality k.

Proof.

(i) Distributivity gives $0a = (0 + 0)a = 0a + 0a$. Adding $-0a$ to both sides gives $0a = 0$.
(ii) Distributivity gives $0 = (-1 + 1)(-a) = (-1)(-a) + (-a)$. Adding a to both sides gives $(-1)(-a) = a$.
(iii) The multiplicative identity and the associativity of multiplication give $na = n(1a) = (n1)a = 0a = 0$.
(iv) We proceed by induction on n. For the base case $n = 0$, we have $(a + b)^n = 1 = \binom{0}{0} a^0 b^0$. The induction hypothesis and the addition identity for binomial coefficients give

$$\begin{aligned}(a + b)^{n+1} = (a + b)(a + b)^n &= (a + b)\left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}\right)\\ &= \left(\sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k}\right) + \left(\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1}\right)\\ &= \sum_{k=0}^{n+1}\left(\binom{n}{k-1} + \binom{n}{k}\right) a^k b^{n+1-k} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k} .\end{aligned}$$ □

2.0.10 Definition. A subset S of a ring R is a ***subring*** if it is a subgroup of R under addition, closed under multiplication, and contains the multiplicative identity 1_R.

The intersection of any family of subrings is a subring. The intersection of all subrings containing a set X is called the ***subring of R generated by X***.

2.0.11 Example. The inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are all subrings. Every subring of the integers $\mathbb{Z}$ or the quotient $\mathbb{Z}/\langle m \rangle$ contains 1 and hence must be equal to the whole ring. ◇

2.0.12 Example. The subset $\mathbb{Z}[\mathrm{i}] := \{a + b\mathrm{i} \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ forms a subring called the ***Gaussian integers***. ◇

2.1 Homomorphisms and Fields

2.1.1 Definition. Let R and S be two rings. A ***ring homomorphism*** is a map $\varphi : R \to S$ such that $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\,\varphi(b)$, and $\varphi(1_R) = 1_S$ for all $a, b \in R$.

A ring is not a group under multiplication (except for the zero ring). If we do not insist that $\varphi(1_R) = 1_S$ then weird things can happen.

2.1.2 Remark. The composition of two ring homomorphism is a ring homomorphism. The methods used to prove Proposition 1.4.6 also establish that a ring homomorphism is isomorphism if and only if it is a bijective homomorphism.

2.1.3 Example. Let R be a ring. The map $n \mapsto n \cdot 1_R$ is the unique ring homomorphism from $\mathbb{Z}$ to R. In particular, the identity map is the unique ring endomorphism of the ring $\mathbb{Z}$. ◇

2.1.4 Example. Complex conjugation $z = a + b\mathrm{i} \mapsto \overline{z} = a - b\mathrm{i}$ is an automorphism of the ring $\mathbb{C}$. ◇

2.1.5 Example. The canonical injection from a subring is a ring homomorphism. ◇

2.1.6 Example. Let R be a commutative ring and let $a \in R$. The ***evaluation map*** $\mathrm{ev}_a : R[x] \to R$ defined by $\mathrm{ev}_a(f) = f(a)$ is a ring homomorphism. ◇

2.1.7 Example. For any element $f \in R[x]$, the substitution $x \mapsto f$ is a ring homomorphism from $R[x]$ to itself. ◇

2.1.8 Definition. A subset I of a commutative ring R is an ***ideal*** if it is an additive subgroup and the relations $r \in R$, $a \in I$ implies $ra \in I$.

2.1.9 Example. For any ring R, both R and $\{0\}$ are ideals. ◇

2.1.10 Example. For any $r \in R$, the set of multiplies of r is an ideal, called the ***principal ideal*** generated by r and denoted by $\langle r \rangle$. ◇

2.1.11 Example. Every intersection of ideals is an ideal; compare with Lemma 1.2.7. For any subset X of a ring R, there exists a unique smallest ideal $\langle X \rangle$ containing X called the ideal ***generated by*** X. ◇

2.1.12 Proposition. *Let* $\varphi : R \to S$ *is a ring homomorphism. The kernel* $\mathrm{Ker}(\varphi) := \{r \in R \mid \varphi(r) = 0\}$ *is an ideal in* R *and* $\mathrm{Im}(\varphi)$ *is a subring of* S. *When* R *and* S *are nonzero rings, we have* $\mathrm{Ker}(\varphi) \neq R$.

Proof. Consider $a \in \mathrm{Ker}(\varphi)$ and $r \in R$. Since φ is homomorphism, we see that $\varphi(ra) = \varphi(r)\,\varphi(a) = \varphi(r)\,0 = 0$, so $ra \in \mathrm{Ker}(\varphi)$. As Proposition 1.4.9 shows that $\mathrm{Ker}(\varphi)$ is an additive subgroup of R, we deduce that $\mathrm{Ker}(\varphi)$ is an ideal. Since $1_R \notin \mathrm{Ker}(\varphi)$, the kernel is a proper ideal whenever R and S are nonzero rings.

For any $a', b' \in \mathrm{Im}(\varphi)$, there are $a, b \in R$ such that $\varphi(a) = a'$, $\varphi(b) = b'$. Hence, we have $\varphi(ab) = \varphi(a)\,\varphi(b) = a'\,b' \in \mathrm{Im}(\varphi)$. Proposition 1.4.9 establishes that the image $\mathrm{Im}(\varphi)$ is an additive subgroup of S containing 1_S, so $\mathrm{Im}(\varphi)$ is a subring. □

2.1.13 Definition. A ring element is a ***unit*** if it has a multiplicative inverse. The set $R^\times$ of all units in a commutative ring R forms an abelian group under multiplication.

2.1.14 Example. We have $(\mathbb{Z}/\langle 6\rangle)^\times = \{1, 5\} \cong \mu_2$ ◇

2.1.15 Proposition. *A formal power series* $f := \sum_{n=0}^{\infty} r_n x^n \in R[[x]]$ *is a unit if and only if the coefficient* r_0 *is a unit in* R.

Proof.
(⇒) If there exists a formal power series $g = \sum_{n\geqslant 0} s_n x^n \in R[[x]]$ such that $fg = 1$, then we have $r_0 s_0 = 1$ so r_0 is a unit in R.
(⇐) Suppose that r_0 is a unit in R. Recursively defining s_n, for all nonnegative integers n, by

$$s_0 := r_0^{-1}\,, s_1 := r_0^{-1}(-r_1 s_0)\,, s_2 := r_0^{-1}(-r_1 s_1 - r_2 s_0)\,, \dots\,, s_n := r_0^{-1}\Big(-\sum_{i=1}^{n} r_i s_{n-i}\Big)\,,$$

it follows that $\left(\sum_{n\geqslant 0} r_n x^n\right)\left(\sum_{n\geqslant 0} s_n x^n\right) = \sum_{n\geqslant 0}\left(\sum_{i\geqslant 0} r_i s_{n-i}\right) x^n\,.$ □

2.1.16 Definition. A ***field*** is a nonzero commutative ring in which every nonzero element is a unit.

2.1.17 Example. Some of our favourite sets of numbers including $\mathbb{Q}$, $\mathbb{R}$,and $\mathbb{C}$ are fields. However, the ring $\mathbb{Z}$ is not a field. ◇

2.1.18 Definition. A ring R is a ***domain*** if its nonzero and the product of two nonzero elements in R is nonzero.

2.1.19 Proposition. *Every field* K *is a domain.*

Proof. If $ab = 0$ and $a \neq 0$, then $b = a^{-1}(ab) = a^{-1}(0) = 0$. □

2.1.20 Proposition. *Any finite domain is a field.*

Proof. Let R be a finite domain and let a be a nonzero element in R. Since R is a domain, the map $x \mapsto ax$ is an injective function. Since R is finite, it is also surjective. In particular, there exists $b \in R$ such that $ab = 1$. Since a was arbitrary, R is a field. □

Combining Propositions 2.1.20 and 2.1.21, we see that $\mathbb{Z}/\langle m\rangle$ is a field if and only if the generator m is a prime number. For a prime number p, the finite field $\mathbb{Z}/\langle p\rangle$ is frequently denoted by $\mathbb{F}_p$.

2.1.21 Proposition. *The quotient ring* $\mathbb{Z}/\langle m\rangle$ *is a domain if and only if the generator* m *of the ideal is a prime number.*

Proof.
(⇐) Suppose that m is prime. Given $q, r \in \mathbb{Z}$ such that $qr \equiv 0 \pmod{m}$, it follows m divides q or m divides r, so either $q \equiv 0 \pmod{m}$ or $r \equiv 0 \pmod{m}$. Hence, the quotient ring $\mathbb{Z}/\langle m\rangle$ is a domain.
(⇒) Suppose that m is not prime. There exists integer q, r such that $m = pq$ and $1 < p, q < m$. It follows that $p, q \not\equiv 0 \mod m$ but $pq \equiv 0 \pmod{m}$. Hence, the quotient ring $\mathbb{Z}/\langle m\rangle$ is not a domain. □